RSAC 2025 Conference

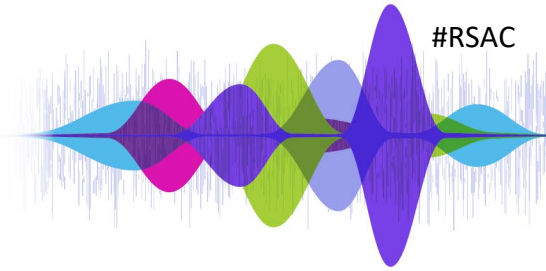
Many Voices.
One Community.

SESSION ID: TPV1-R02

The Dark Side of SOC 2: Third-Party Risks Hiding in Plain Sight

Mike Kerem
CTO
TrustNet

Trevor Horwitz
CISO
TrustNet



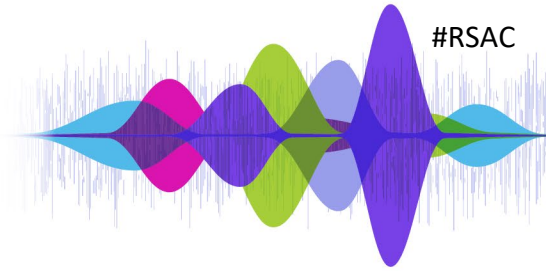
Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

Goals for this session



- **Enhance** your ability to identify hidden weaknesses in SOC 2
- **Improve** your understanding of SOC 2 impacts
- **Strengthen** your expertise in mitigating SOC 2 risks

If you only knew the power of the Dark Side.

SOC 2 Essentials

Purpose: Evaluate an organization's controls related to **security, availability, processing integrity, confidentiality, and privacy** (Trust Services Criteria)

Who Needs It:

- Any organization providing mission-critical services or storing, managing, processing handling sensitive data
- Examples: SaaS providers, technology and cloud providers, B2B service providers

Issued By: Certified public accounting (CPA) firms after an independent audit

Framework: Based on **AICPA's Trust Services Criteria (TSC)**

SOC 2 Essentials

Types of Reports:

- **SOC 2 Type 1 –** point-in-time assessment
- **SOC 2 Type 2 –** over a period (typically 3-12 months)

Key Report Components:

- Independent audit opinion
- Management assertion
- System scope and description
- Testing and results

SOC 2 Essentials

Why It Matters: Provides assurance to customers and stakeholders that systems are secure and properly managed

Commonly Used For:

- Service Provider due diligence and risk assessments
- Compliance requirements
- Demonstrating security posture

RSAC™ 2025 Conference

An in-depth look at hidden risks

There are no issues with our SOC 2 report.
Move along. You can go about your business.

Misaligned Scope and Controls

Issue: Scope is defined by a “system” boundary

Risks:

- System boundary misunderstood
- Critical systems excluded

Example: SOC 2 addresses only **one product** or line of business

Why It Matters:

- Scope excludes some of the Service Provider's infrastructure
- Out-of-scope systems not audited

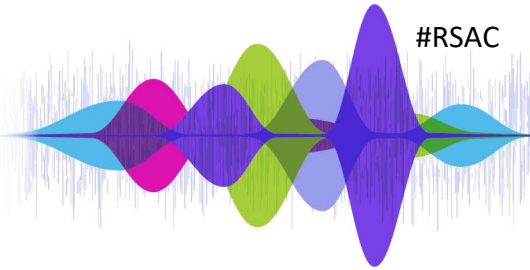
Misaligned Scope and Controls

Actionable Insights:

- **Review the System Description**
- Service Provider disclosure of **out-of-scope systems**
- **Additional evidence** for out-of-scope components

Assume nothing is in scope unless explicitly stated

Overlooked Subservice Supply-Chain Risk



Issue: **Subservice organizations** may have weak security

Risk:

- Weak controls **cascade** into hidden risks
- **Assumptions** go unchecked
- Third/fourth party **hidden vulnerabilities**

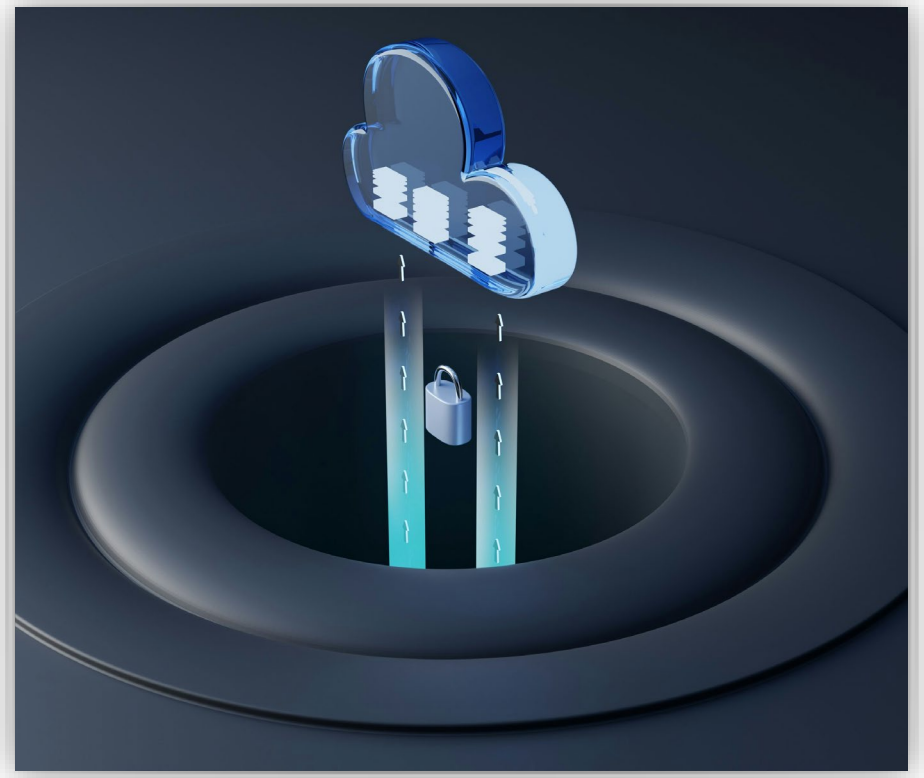
Example: A SaaS Service Provider relying on a CSP cloud with weak security introduces a hidden vulnerability

Overlooked Subservice Supply-Chain Risk

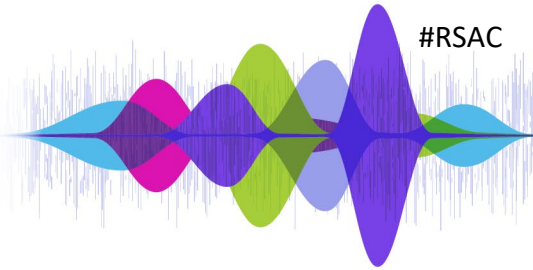
Why It Matters: Service Providers may inherit weak security or neglect security best practices

Common oversights include:

- **Misconfigured cloud settings** (S3 buckets, IAM policies)
- **No monitoring and logging** of subservice provider activity
- **Over-reliance on default security settings** without independent verification



Overlooked Subservice Supply-Chain Risk



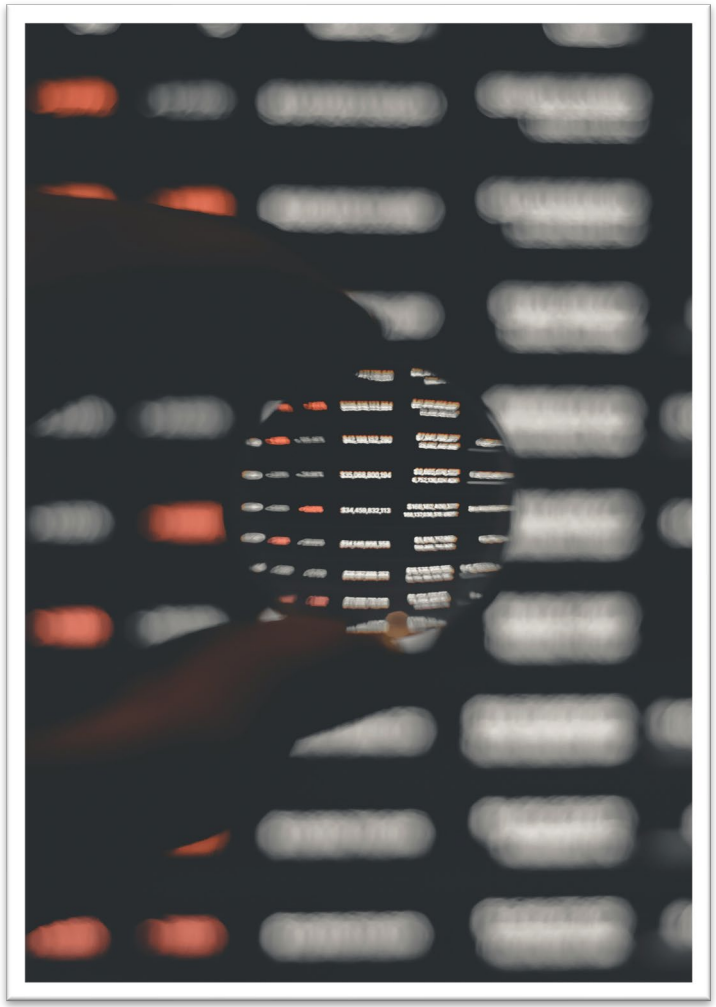
Actionable Insights:

- **Identify subservice providers** (see System Description)
- Ensure Service Providers' **risk assessments** on subservice providers are robust
- Validate subservice providers are monitored (e.g., CSPM, audits, pentests)
- Evaluate controls and **SOC 2 report** for carveouts

Controls are only as strong as the weakest subservice provider

Verify inherited security

Absence of Specific Security Domains



Issue: Trust Service Criteria (TSCs) are not mandatory:

- **Security** (core controls, always required)
- **Availability** (system uptime and reliability)
- **Confidentiality** (sensitive data protection)
- **Processing Integrity** (accuracy and reliability)
- **Privacy** (manage personal data)

Critical controls may be excluded

Risk: Missing controls create **inherited risks**

Example: Service Provider omits confidentiality and **sensitive customer data** is not protected

Absence of Specific Security Domains

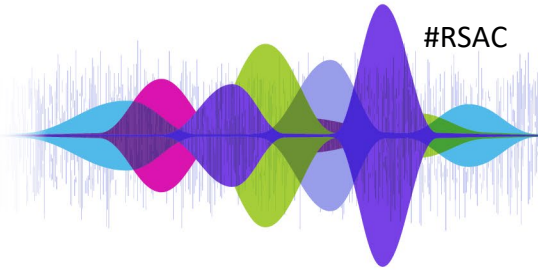
Why It Matters:

- SOC 2 may not address **your** critical risks

This may lead to:

- **Compliance gaps** – mishandled personal data, unmet regulations
- **Reliability risks** – downtime or data corruption risks
- **Weak data protection** – unclear encryption, retention, and deletion practices

Absence of Specific Security Domains



Actionable Insights:

- **Missing TSCs** may signal risks
- **Investigate excluded criteria** and consider alternative assurances
- **Cross-map controls** and identify potential gaps
- **Request supporting docs:** PIAs, uptime reports, data validation

Inherited insecurity

Continuous Security Not Guaranteed

Issue: **Historical audits** don't guarantee post-audit security changes

Risks: SOC 2 assurance may be ambiguous due to:

- **Post-audit security incidents**
- **Key personnel changes**
- **Infrastructure changes** (new CSPs and third parties)
- **Evolving compliance requirements**

Continuous Security Not Guaranteed

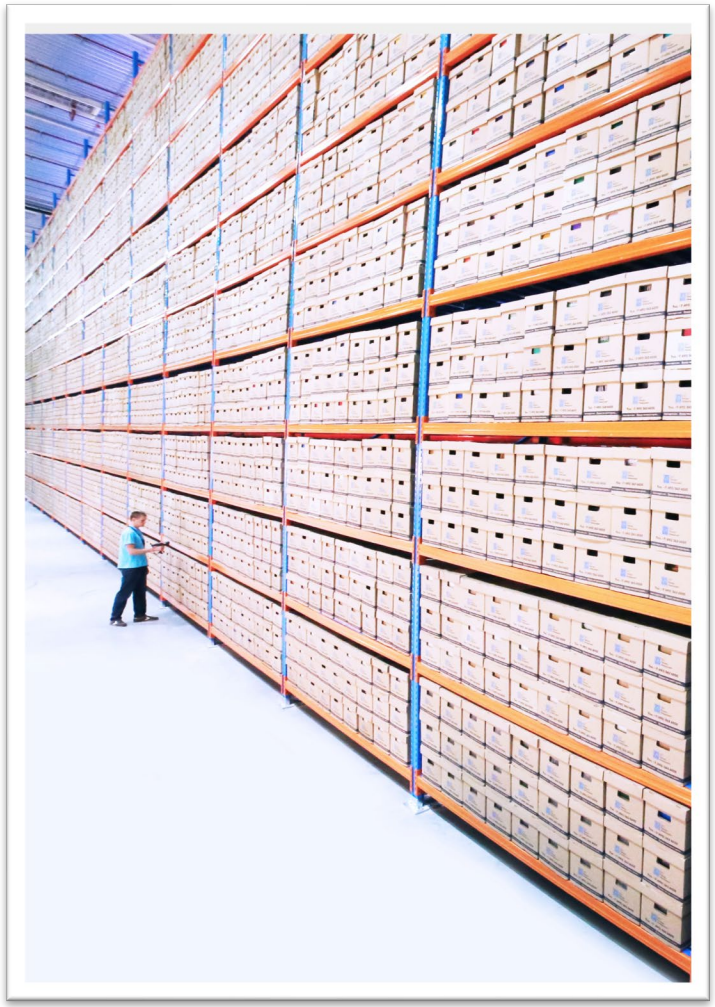
Example:

Post-audit events:

- A ransomware attack
- Outsourced security
- New subservice provider

Relying only on SOC 2 reports may miss evolving security risks

Continuous Security Not Guaranteed



Why It Matters:

Overreliance on audit snapshots, assuming ongoing security

Audits may miss:

- Post-audit vulnerabilities
- Security control changes
- Subsequent breaches or compliance failures

Ongoing monitoring can uncover previously hidden risks

Continuous Security Not Guaranteed

Actionable Insights:

- Develop transparent and trusted Service Provider relationships
- Assess recent incidents and major changes
- Continuous monitoring (iTrust, BitSight, SecurityScorecard)
- Require periodic security updates and prompt incident disclosures (SLAs, contracts)
- Supplement SOC 2 with questionnaires, pentests, and compliance reviews

SOC 2 is just a snapshot – manage Service Provider risk with continuous monitoring and transparency

Controls Vary Significantly Between Service Providers

Issue: SOC 2 focuses on objectives, not specific controls - report quality dependent on:

- **Service Provider's scope**
- **Audit rigor**
- **Service Provider's security program maturity**

Not all SOC 2 reports provide the same level of assurance

Controls Vary Significantly Between Service Providers

Risks:

- **Superficial audits:** minimal checks from low-quality audits
- **Scope manipulation:** risky systems excluded
- **Dissimilar assurance:** Service Providers have different security postures

Controls Vary Significantly Between Service Providers

Example: Service Providers have **SOC 2 Type 2 reports**, but:

- **Service Provider A** has a mature security program with 24/7 monitoring and regular testing
- **Service Provider B** meets minimum standards, lacks real-time detection, and skips testing simulations

Controls Vary Significantly Between Service Providers

Why It Matters:

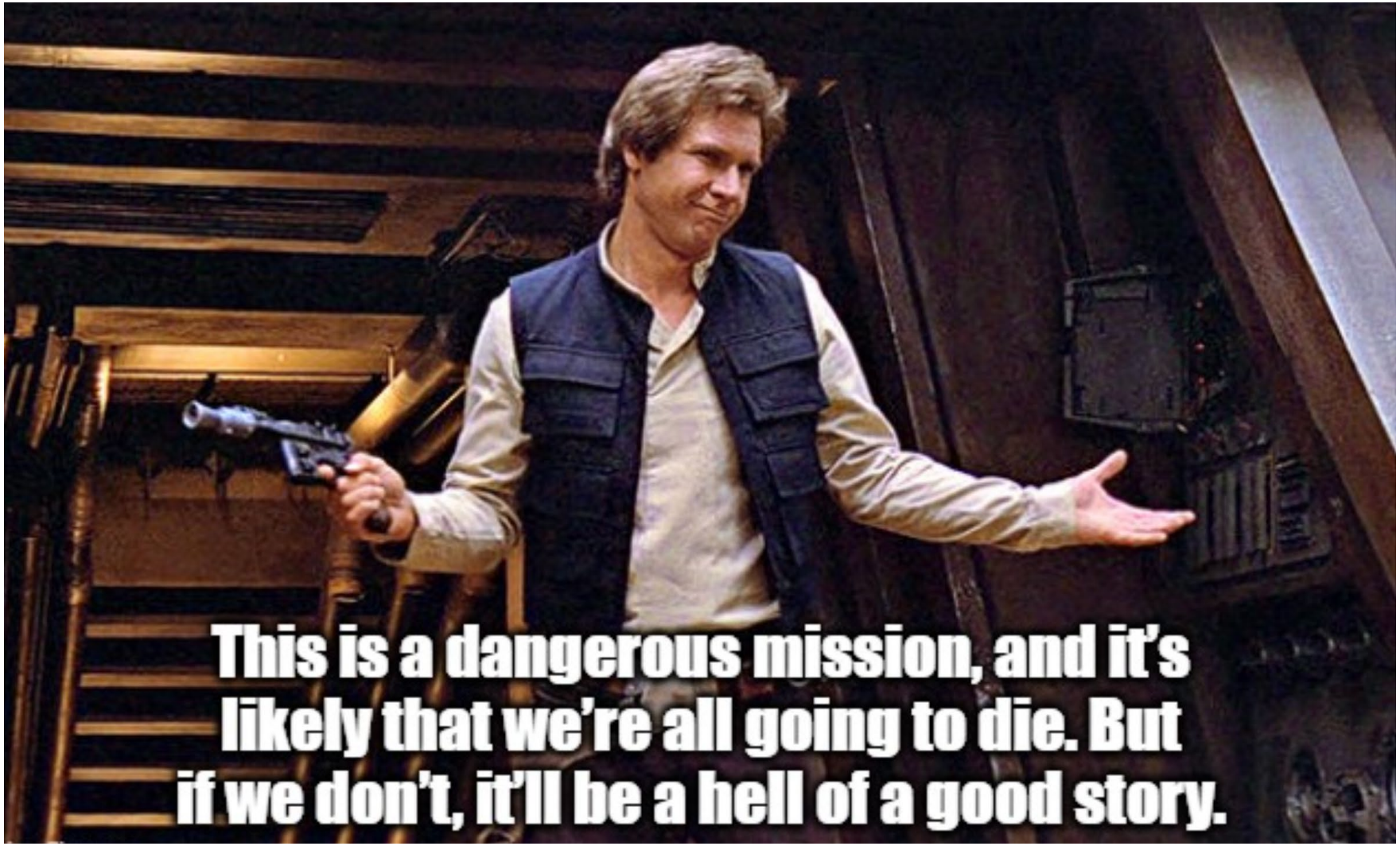
- SOC 2 is an **attestation, not a certification**
- Service Providers control the auditor, scope, and (indirectly) rigor
- Weak SOC 2 reports offer false confidence
- Poor audit quality overlooks inadequate controls
- Inadequate testing leads to critical blind spots

Controls Vary Significantly Between Service Providers

Actionable Insights:

- **Auditor credibility** – reputable, deep cybersecurity skills
- **Review scope** – for carve-outs or limited coverage exclusions
- **Assess control depth** – best practices like MFA, pentests, incident response drills
- **Compare security maturity** – inquire about monitoring, response, and remediation
- **Supplement gaps –** with other security reviews and monitoring

Not all SOC 2 reports are equal — dive deeper


This is a dangerous mission, and it's
likely that we're all going to die. But
if we don't, it'll be a hell of a good story.

Unrealistically Perfect SOC 2 Reports

Issue:

A flawless SOC 2 report may signal a narrow scope, weak auditing, or poor transparency

Risks:

- **False confidence** - zero findings may mask scope issues
- **Missed risks** - no findings ≠ no vulnerabilities
- **Lack of transparency** - no exceptions may hide remediation gaps
- **Scope manipulation** – squeaky clean reports may exclude high-risk areas

Unrealistically Perfect SOC 2 Reports

Example: A SOC 2 report with minor gaps and documented fixes shows strong auditing and Service Provider maturity

Why This Matters:

- Transparent remediation builds more trust than a “perfect” report
- Focus on how Service Providers handle issues—not just the lack of findings
- Ongoing improvement is more valuable than assumed flawlessness

“No-exception” SOC 2 may signal weak audits or limited scope.

Unrealistically Perfect SOC 2 Reports

Actionable Insights:

- Question clean reports—ask about issue handling and improvements
- Request remediation details—review past gaps and fixes
- Evaluate risk maturity—check how issues are managed beyond audits
- Look beyond SOC 2—use pentests, monitoring, and questionnaires
- Choose transparent providers—those who own and fix issues build trust

Build strong Service Provider relationships to ensure transparency

Shared Security Roles

Issue: Complementary User Entity Controls (CUECs), define shared security duties—missing them creates gaps

Risks:

- Misconfigs can cause breaches
- Weak access controls enable unauthorized access
- No backups = data loss
- Incorrectly assume the Service Provider handles all security

Example: SaaS provider manages authentication, but misconfigured RBAC, missing MFA, or open APIs remain customer risks

Shared Security Roles

Why This Matters: **Security is a shared responsibility.** Customers must implement harmonizing controls to stay protected.

Actionable Insights:

- Review SOC 2 CUECs and map them to internal controls
- Follow Service Provider config, logging, and monitoring best practices
- Conduct regular internal audits/reviews to ensure CUEC compliance
- Train personnel to manage and maintain security controls

RSAC 2025 Conference

Session Recap and Takeaways

Many Voices.
One Community.

Key Takeaways

Align scope and controls with real risks

- Cross-check System Description with service offering
- Identify and validate excluded systems or business units
- Prioritize mission-critical providers with modular services (separate products or regions)

Actively identify and manage subservice provider risks

- Identify subservice providers; request their SOC 2
- Review onboarding and monitoring of subservice providers
- Flag service providers using cloud or major third-party services for critical risk reviews

Absence of Specific Security Domains

- Map TSCs to your risks and collect alternate proofs if mapped risks are missing
- Ask why domains were excluded; ensure alignment with your risks
- Prioritize providers handling PII, payments, or regulated data

Key Takeaways

Supplement SOC 2 audits with continuous security monitoring

- Check audit period and report date
- Require disclosure of all security incidents
- Use tools (iTrust, SecurityScorecard, BitSight) for continuous monitoring

Evaluate the Service Provider's unique control strength

- Validate auditor's credentials and independence
- Compare controls rigor across providers
- Ask about security maturity indicators (IR plans, MDR, SLAs)
- Prioritize providers with weak reports or unknown auditors

Key Takeaways

Ensure reports acknowledge and address real-world issues

- Question zero-exception reports; request remediation evidence
- Look beyond SOC 2—use pentests, monitoring, and questionnaires
- Escalate reviews for “clean” reports with a weak history

Clarify shared security responsibilities to avoid gaps

- Review and assess Complementary User Entity Controls (CUECs) in each report
- Ensure proper internal config (MFA, RBAC, APIs)
- Conduct audits and training on shared responsibilities
- Prioritize vendors with configurable platforms and shared controls

FEAR IS THE PATH TO THE DARK SIDE.

Q&A

RSAC™ 2025 Conference

Many Voices.
One Community.

Download the

SOC 2 Evaluation Checklists

www.TrustNetInc.com/TrustNet-RSAC-2025